Listing of the Claims:

The listing of claims below will replace all prior versions and listings of claims in this Application.

1. (original) A method of securing electronic data, the method comprising:

receiving electronic data;

receiving a selection of one of a plurality of digital rights management systems; and

encrypting the data in accordance with the selected digital rights management system.

2. (original) The method of Claim 1, wherein receiving electronic data comprises receiving data encrypted according to a first digital rights management system, wherein the first and selected digital rights management systems are different.

3. (original) The method of Claim 2, further comprising decrypting the received electronic data according to the first digital rights management system.

4. (original) The method of Claim 1, further comprising receiving a selection of one of a plurality of compression techniques, and reformatting the received electronic data in accordance with the selected compression technique.

5. (original) The method of Claim 4, wherein a consumer selects the digital rights management system and the compression technique.

6. (original) The method of Claim 4, wherein an operator selects the digital rights management system and the compression technique.

7. (original) The method of Claim 4, wherein a software module is configured to select the digital rights management system and the compression technique.

8. (original) A method of securely distributing digital content, the method comprising:

receiving a plurality of digital data files, the files utilizing a plurality of different file format types;

receiving a selection of a plurality of file format types;

reformatting the files in accordance with the format types;

receiving a user selection of a first digital rights management system, the first digital rights management system being one of a plurality of pre-determined digital rights management systems;

encrypting the reformatted files according to the selected digital rights management system; and

transmitting the encrypted files to a plurality of consumers.

9. (original) The method of Claim 8, wherein at least one of the received files is protected by a second digital rights management system, and further comprising decrypting the at least one file in accordance with the first digital rights management system prior to reformatting the at least one file.

10. (original) The method of Claim 8, further comprising dynamically creating at least one of a format object or a writer object corresponding to the file format types of the received files and the selected file format types, and wherein reformatting the files comprises using the dynamically-created format object or writer object to reformat the files.

11. (original) A method of encoding data with one of a plurality of digital rights management systems, the method comprising:

receiving an identifier of an input file, the input file containing input data;

determining a first file format type used in the input data, the first file format type being one of a plurality of pre-determined file format types;

receiving an identifier of a first digital rights management system, the first digital rights management system being one of a plurality of pre-determined digital rights management systems;

retrieving unencrypted data from the input file;

encrypting the unencrypted data according to the first digital rights management system;

receiving an identifier of a second file format type for use in an output file, the second file format type being one of a plurality of pre-determined file format types; and

creating the output file according to the second file format type, wherein the output file contains the encrypted data.

12. (original) The method of Claim 11, further comprising determining a first compression format used in the input file.

13. (original) The method of Claim 12, wherein retrieving unencrypted data comprises decompressing compressed data from the input file according to the first compression format.

14. (original) The method of Claim 12, further comprising (i) receiving an identifier of a second compression format to be used in the output file, the format being one of a plurality of pre-determined compression formats, (ii) compressing the unencrypted data according to the second compression format, and (iii) encrypting the compressed unencrypted data.

15. (original) The method of Claim 11, further comprising receiving an identifier of a second digital rights management system used in the input file, the second digital rights management system being one of a plurality of pre-determined digital rights management systems.

16. (original) The method of Claim 15, wherein retrieving unencrypted data from the input file comprises decrypting the input data according to the rules of the second digital rights management system.

17. (original) The method of Claim 11, further comprising generating digital rights management system rules, and writing the generated digital rights management system rules to the output file according to the first digital rights management system.

18. (original) The method of Claim 15, further comprising (i) retrieving digital rights management system rules from the input file, (ii) mapping the retrieved digital rights management rules to rules in accordance with the first digital rights management system, and (iii) writing the mapped rules to the output file.

19. (currently amended) A method of handling secured electronic data, the method comprising:

receiving electronic data encrypted according to a first digital rights management system;

receiving a selection of one a plurality of digital rights management systems to be applied to the data, wherein the first digital rights management system and the selected digital rights management system are different;

decrypting said electronic data; and

re-encrypting said electronic data in accordance with said selected digital rights management system.

20. (original) The method of Claim 19, wherein the first and the selected digital rights management systems differ in that each uses different data encryption from the other.

21. (original) The method of Claim 20, further comprising decompressing the received data according to a first compression technique and recompressing the decompressed received data according to a second compression technique.

22. (original) The method of Claim 21, further comprising converting the data from a first file format type to a second file format type, wherein the second file format type is compatible with the selected digital rights management system.

23. (original) A system for protecting digital presentations with a digital rights management system, the system comprising:

a first storage device storing an input data file;

a second storage device;

a translation computer;

a digital rights management system encryption library, accessible by the translation computer, the encryption library comprising a plurality of classes, each class configured to create a software module configured to encrypt data according to a particular digital rights management system;

a file format type library, accessible by the translation computer, the file format type library comprising a plurality of classes, each class configured to create a software module configured to read data using a different file format type;

a file writer library, accessible by the translation computer, the file writer library comprising a plurality of classes, each class configured to create a software module configured to write to a different file format type; and

a driver module configured to:

determine a first file format type of the input file;

obtain input data from the input file using a file format class corresponding to the first file format;

select a first digital rights management encrypting class from the plurality comprising the digital rights management systems library;

encrypt the input data according to the first digital rights management system encrypting class;

determine a second file format type for a data output file; and

write the data output file containing the newly-encrypted data to the second storage device using a file writer class corresponding to the second file format type.

24. (original) The system of Claim 23, further comprising:

a compression format library, accessible by the translation computer, the compression format library comprising a plurality of classes, each class configured to create a module configured to compress data according to a particular compression technique;

a decompression format library, accessible by the translation computer, the media decompression format library comprising a plurality of classes, each class configured to create a module configured to decompress data according to a particular decompression technique; and

the driver module being further configured to:

determine a first compression format used by the input file;

decompress the input data using a decompression class corresponding to the first compression format;

determine a second compression format for use by the output file; and

compress the input data using a compression class corresponding to the second compression format.

25. (original) The system of Claim 23, further comprising:

a digital rights management decryption library, accessible by the translation computer, the decryption library comprising a plurality of classes, each class configured to create a module configured to decrypt media content according to a particular digital rights management process, and the driver being further configured to (i) determine a second digital rights management system used by the input file, and (ii) decrypt the input data using a digital rights management decryption class corresponding to the second digital rights management system.

26. (original) The system of Claim 23, further comprising a digital rights rules library, accessible by the translation computer, the digital rights rules library comprising a plurality of classes, each class comprising a plurality of data access rules compatible with the first digital rights management system.

27. (original) A computer readable medium containing instructions which, when executed, perform the method comprising:

receiving an identifier of an input file, the input file containing input data;

determining a first file format type used in the input file, the first file format type being one of a plurality of pre-determined file format types;

receiving an identifier of a first digital rights management system, the first digital rights management system being one of a plurality of pre-determined digital rights management system;

retrieving unencrypted data from the input data file;

encrypting the unencrypted data according to the first digital rights management system;

receiving an identifier of a second file format type, the second file format type being one of a plurality of pre-determined file format types; and

creating an output file according to the second file format type, wherein the output file contains the encrypted data.

28. (original) The computer readable medium of Claim 27, further comprising instructions, which, when executed, determine a first compression format used in the input file, and

wherein retrieving unencrypted data from the input file comprises decompressing compressed data from the input file according to the first compression format.

29. (original) The computer readable medium of Claim 28, further comprising instructions, which, when executed, perform the steps of:

receiving an identifier of a second compression format, the second compression format being one of a plurality of pre-determined compression formats;

compressing the unencrypted data according to the second compression format; and

wherein encrypting the unencrypted data comprises encrypting the compressed unencrypted data.

30. (original) The computer readable medium of Claim 27, further comprising instructions, which, when executed, perform the steps of:

receiving an identifier of a second digital rights management system, the second digital rights management system being one of a plurality of pre-determined digital rights management systems, wherein retrieving unencrypted data from the input file comprises decrypting input data according to the rules of the second digital rights management system

31. (original) The computer readable medium of Claim 27, further comprising instructions, which, when executed, perform the steps of generating digital rights management rules, and writing the generated digital rights management rules to the output file.

32. (original) The computer readable medium of Claim 30, further comprising instructions, which, when executed, perform the steps of:

retrieving digital rights management rules from the input file;

mapping the retrieved digital rights management rules according to rules of the first digital management system; and

writing the mapped digital rights management rules to the output file.